CLAIMS

1. A method of managing security keys in a wireless local area network having a mobile terminal, an access point and a server, the method comprising the steps of:

obtaining first and second certificates from a certificate authority;

associating the mobile terminal with the access point;

using a certificate authority certificate, first certificate and private key with Internet Key Exchange (IKE) to generate a a WLAN link level key and mutually authenticating the mobile terminal and the access point using the IKE; and

using a certificate authority certificate, second certificate and private key with Internet Key Exchange (IKE) to generate IPsec authentication, encryption and decryption keys for data packets

transferred between the mobile terminal and the server.

2. The method recited in claim 1, wherein the certificate authority certificate, private key, and the first and second certificates are stored in the mobile terminal.

3. The method recited in claim 2, wherein the certificate authority certificate, private key, and the first and second certificates are stored in the mobile terminal at the time of manufacture of the mobile terminal.

4. The method recited in claim 1, wherein the mobile terminal generates an authentication header for transferred data packets utilizing the IPsec encryption key.

5. The method recited in claim 1, wherein the server authenticates and decrypts data packets transferred from the mobile terminal utilizing the IPsec authentication and decryption keys.

6. The method recited in claim 5, wherein the data packets are transferred from the mobile terminal to the access point using WLAN link level encryption in addition to the IPsec encryption.

7. The method recited in claim 6, wherein the WLAn link level encryption comprises Wired Equivalent Pricay (WEP) encryption.

8. The method recited in claim 1, wherein the data packets are transferred from the mobile terminal to the access point without using WLAN link level encryption.

9. The method recited in claim 8, wherein the mobile terminal forwards the IPsec authentication key to the access point.

10. The method recited in claim 9, wherein the access point authenticates data packets from the mobile terminal using the IPsec authentication key forwarded from the mobile terminal.

11. The method recited in claim 1, wherein the mobile terminal sends an IPsec authenticated message to an access point as part of a MAC-level message of the wireless local area network.

12. A method for use in a wireless local area network (WLAN) in which MAC-level messages are transferred between mobile terminals and access points associated with the mobile terminals, said method comprising the steps of:

generating an IPsec authentication header in a mobile terminal; and

including said IPsec authentication header in a MAC-level message transferred from the mobile terminal to an associated access point.

13. The method recited in claim 12, wherein the mobile terminal includes a WLAN control process and an IPsec kernel.

14. The method recited in claim 13, wherein the IPsec kernel builds the authentication header and passes it to the WLAN control process.

15. The method recited in claim 12, wherein the access point includes an IPsec kernel and a WLAN control process.

16. The method recited in claim 15, wherein the WLAN control process determines that the MAC-level

message contains IPsec authenticated data and extracts that data from MAC-level message.

17. The method recited in claim 16, wherein the WLAN control process authenticates the MAC-level message.